At-A-Glance

Environment

- Data Center and Cloud Service Provider
- Transmits data to more than 1600 peered networks around the world
- DDoS attacks wreaking havoc on the network

Challenge

Deliver highly available services to global clients in spite of nonstop DDoS attacks

Extreme Solution Components

- Extreme MLXe Routers for core routing
- Extreme NetIron CER 2000 Series Routers deployed as backup

Results

- Deployed 700 gigabytes of capacity across a global network infrastructure
- Delivers clean traffic with minimal latency or rerouting across the network
- Successfully mitigates hundreds of DDoS attacks daily

Massively Scalable Routers Protect Global Network Traffic Against DDoS Attacks

This Australian-based data center and cloud service provider (CSP) hosts hundreds of thousands of Internet Web sites and cloud services for local, national, and international businesses and government agencies. It securely transmits data to more than 1600 peered networks around the world every day. Core business services range from basic Web hosting to cloud services, disaster recovery solutions, security surveillance, and many others. But one of its best-known capabilities is its Distributed Denial of Service (DDoS) protection, which helps keep clients' Web sites running smoothly.

Solving a Massive Challenge

When the CSP first began offering services, it used a Cisco platform. As the company grew, the more attractive it became as a target for cyber terrorists. Suddenly, DDoS attacks were bringing the network to its knees, and the CSP team had no idea where the traffic was coming from. After enabling NetFlow, the team could see source and destination data. However, when an attack occurred, network routers could not provide source and destination data while also passing traffic.

"We wanted massive routers with massive capacity and the ability to show us source and destination so that we could control network flows," said the Managing Director. "We chose Extreme Networks MLXe Routers so that we can route large amounts of unwanted traffic and survive the very worst possible day."

Growing Globally

In 2010, the CSP deployed its first Extreme MLXe Routers in its data centers, connected over point-to-point dark fiber. Now it could roll out high-availability, geographically redundant IP services for mission-critical hosting. The team could simultaneously monitor and pass traffic during a DDoS attack and then normalize the unwanted traffic to avoid affecting other clients. Rapid growth continued, and they continued to deploy MLXe Routers. In 2014, the company expanded internationally, purchased more Extreme MLXe Routers, and also invested in anti-DDoS hardware, which was deployed in the United States and Australia.

"For the most effective DDoS protection, we want to be as close to the attack source as possible. We also want to connect to as many networks as possible so we can control the flow of inbound traffic when our customers are under attack."

Now they had the capacity to absorb an attack and the technology to clean Australian traffic within Australia and clean international traffic in the United States. This approach worked better, but during a DDoS attack, traffic comes from all over the world to a single location. The CSP expanded its network again to deploy scrubbing centers in Amsterdam, Singapore, Los Angeles, Sydney, and Melbourne.

Their locations are connected over a global Multiprotocol Label Switching (MPLS) network for optimal routing of clean traffic across regions. Extreme MLXe Routers reside at the network edge, in front of DDoS mitigation systems, load balancers, and firewalls in each location. Extreme CER 2000 Series Routers provide backup designated router (BDR) functionality if required.

Clean and Connected

They deliver one of the most connected networks in Australia. The latest implementation of Extreme solutions increased network capacity to 700 gigabytes and extended the company's reach to global customers. This infrastructure enables them to deliver tiered service offerings, such as remote protection for Web sites and online resources or network-based protection with Soak & Scrub services. Domestic traffic within each scrubbing region is cleaned within the region—as close to the source as possible. This ensures that only clean traffic travels across the network while minimizing latency and avoiding the need to reroute international traffic.

Massive Mitigation

With a highly fault-tolerant site infrastructure, they can now addresses large DDoS attacks. Their Director says that attackers are always devising new ways to increase their impact. A recent attack directed traffic at 90 Gbps against a client. Another attack launched 3 Gbps against another client, but originated entirely within Australia on a Tier 1 provider's network.

"Whether a DDoS attack is 90 Gbps or 3 Gbps, our network absolutely handles it. We successfully mitigate hundreds of attacks daily."

Heading for Tier IV

To date, they have experienced 30 percent growth per year, and it expects that rate of growth to continue. With a blue-chip client list, they are now building Australia's first Tier IV-certified data center and aims to complete construction and certification in 2017. Thanks to Extreme, its traffic will be protected.

"When it's finished, we will have the best datacenter in Australia from a power, cooling, and network point of view. Our clients—whether small businesses or large hosting companies and global enterprises—will not only continue to receive highly available services, they'll also have some of the most advanced DDoS protection available."